Capt Alamri, 2Lt Hayden, 2Lt Mireles

Lab 2 – Scanning

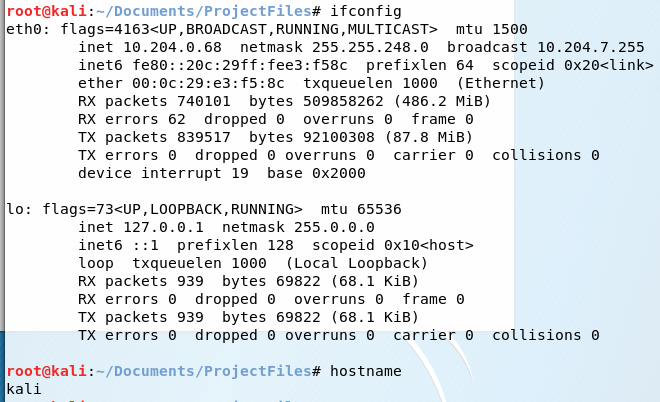
Dr. Mullins

1/16/2019

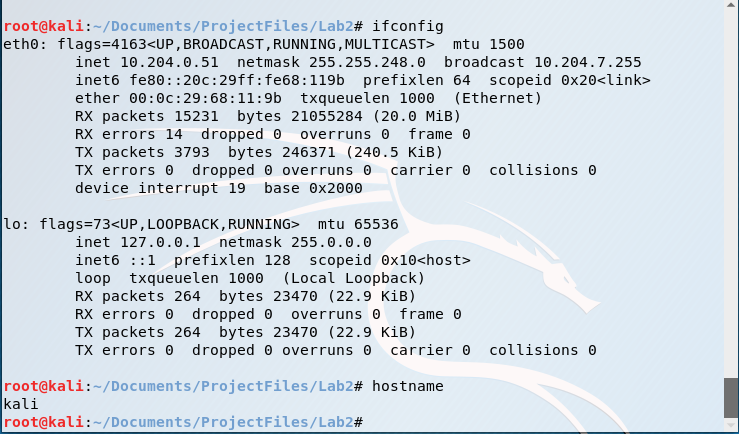
**Network Mapping**:

1. What is the IP address and host name of your machine? What is the IP address and host name of your partner’s machine?

* My IP address is 10.204.0.68, with a hostname kali

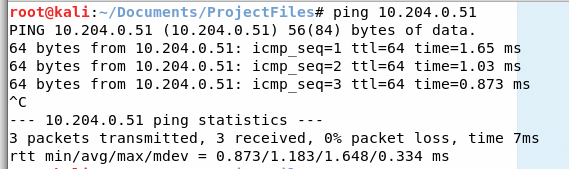


* My partner’s IP address is 10.204.0.51, with a hostname of kali

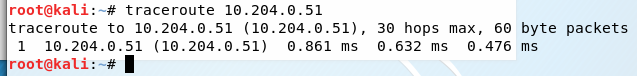


1. Using ping, determine if your partner’s workstation is up. Is your partner’s workstation up?

* My partner’s workstation is working because I received responses back from 10.204.0.51  
  because all packets sent were received.



1. Using tracert, determine the number of hops between your two machines. How many hops are there between the two computers?

* There is one hop between the two computers.

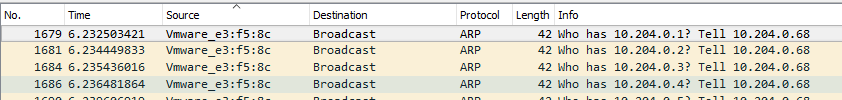
1. Perform a network sweep using arp-scan to identify potential targets/IPs quickly.

What type of packet is the tool sending? Provide a Wireshark screenshot showing some of the captured packets.

How many IPs did the tool discover?

Did the tool scan sequentially? What does the third column represent, and how is that information learned?

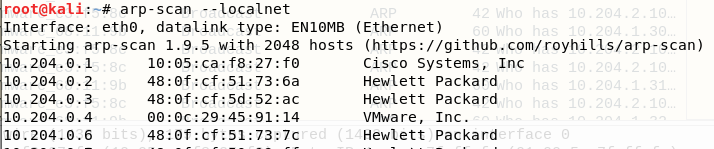
* The packets sent are link-layer ARP broadcasts, sent from my machine at 10.204.0.68.



* The tool discovered 56 hosts (it received 56 responses) out of 2048 hosts scanned.



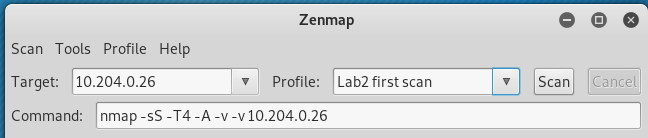
* The tool scanned sequentially, incrementing the target IP by one each iteration. As shown above boxed in yellow, the first packet was to 10.204.0.1, followed by 10.204.0.2, etc.
* The third column of the arp-scan contains the manufacturer(s) details, shown in the arp-scan result below. This information is learned by analyzing the first 3 bytes of the MAC address shown in column 2.



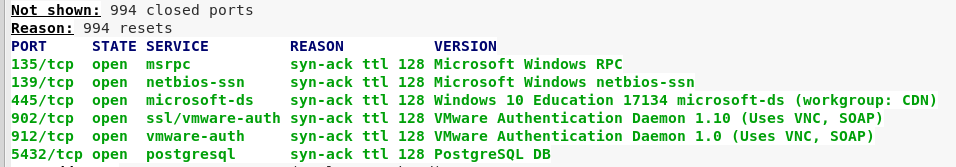
**Nmap**

1. Blackhat: Start Wireshark and perform a SYN scan using nmap or zenmap. Use aggressive timing and turn on verbose output. You may add other options as needed to provide the following information about the target. Using just the nmap results, answer the following questions; in other words, you cannot ask your partner for the name of his/her machine.
   1. What nmap command did you use? Describe all options used and how they affect the scan.

* The nmap command is shown below, boxed in red.



* -sS is a SYN scan
* -T4 indicates aggressive timing
* -A enables all advanced/aggressive options
* -v -v sets the verbosity level to 2
* 10.204.0.26 is the target’s IP address.
  1. Which ports are open? Provide a screenshot.  
     There are 6 open ports: 135, 139, 445, 902, 912, 5432



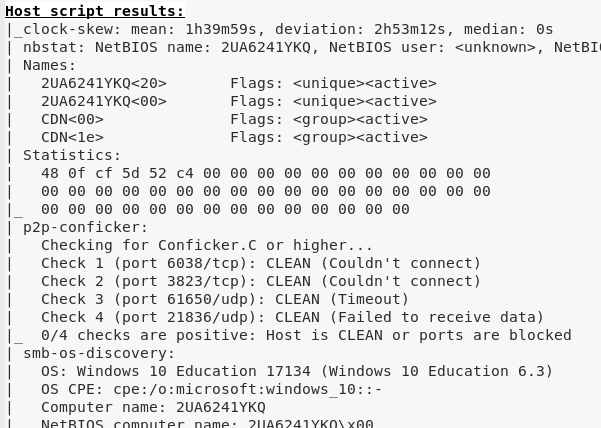
* 1. What services are being offered? Spell out all acronyms.

The services offered for the ports above are:

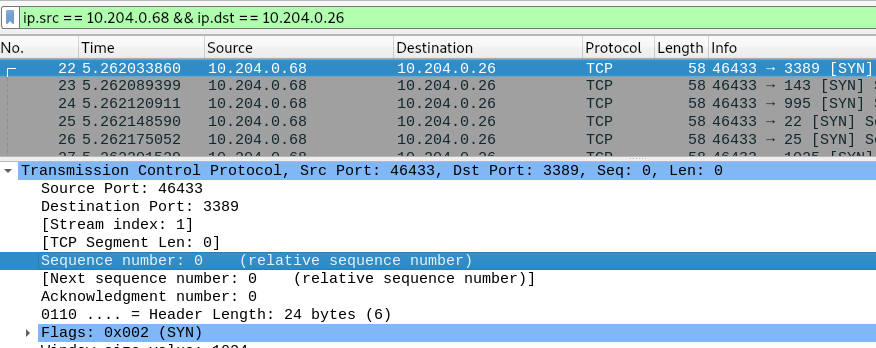
* msrpc – Microsoft remote procedure call
* netbios-ssn – NETBIOS session service
* Microsoft-ds – Microsoft directory services
* ssl/vmware-auth – secure sockets layer, vmware-authorization
* vmware-auth – vmware authorization
* postgresql - PostgreSQL is a open source object-relational database system  
  1. What is the MAC address?
* The MAC address is 48:0F:CF:5D:52:C4



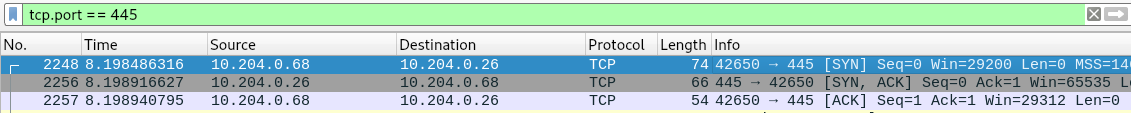
* 1. What is the operating system?
* The operating system is Windows 10 Education 17134, outlined below in red.



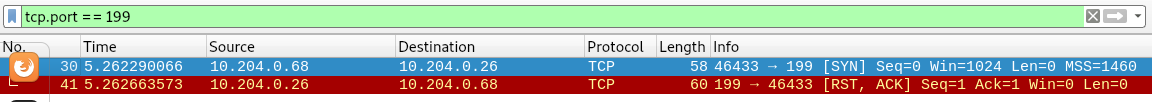
* 1. What is the hostname of the target (e.g., LISXP33LG)?
* The hostname is 2UA6241YKQ, outlined above in yellow.  
  1. Look at the Wireshark data. During the scans, what type of packets did your workstation send to the target (i.e., which flags are set in the packets)?
* The packets are TCP packets with the SYN flag set, as shown below highlighted in red, as well as the hex value of the Flag field as 0x002.



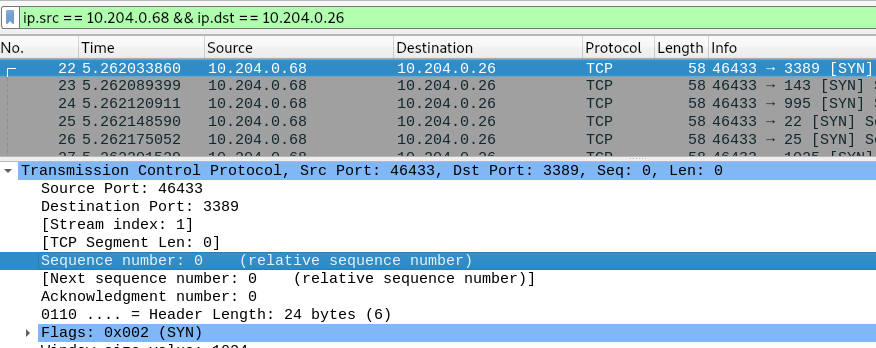
* 1. Select a port listed as open by nmap. How did the target respond for the open port? How did the Blackhat computer respond to the target’s response? Provide a screenshot of your filtered results. Useful filter: **tcp.port == <port #>**
* The target responded with a TCP SYN-ACK packet
* The Blackhat computer responded with an TCP ACK packet, completing the 3-way handshake



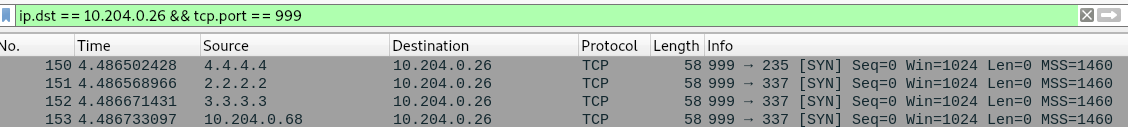
* 1. Select a port listed as closed by nmap. How did the target respond for the closed port? Provide a screenshot of your filtered results.
* The target responded with a TCP RST-ACK packet, indicating the target was not expecting the packet.



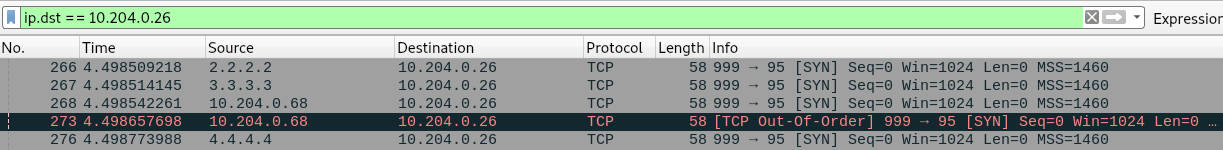
* 1. Were the ports scanned sequentially?
* No, the ports were not scanned sequentially. As shown below, port 3389 preceded 143, 995, 22, and 25 respectively.



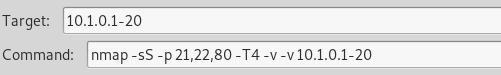
1. Now try nmap’s decoy feature.  
   Blackhat: Start Wireshark and run a SYN scan against ports 1-500 with decoy addresses of **2.2.2.2, 3.3.3.3, <<your real IP>>, 4.4.4.4**. Note there is no space between those addresses, just a comma. Also set your source port number to 999.
   1. Provide a screenshot of the Wireshark screen demonstrating the decoy and real IP addresses along with the 999 port number.



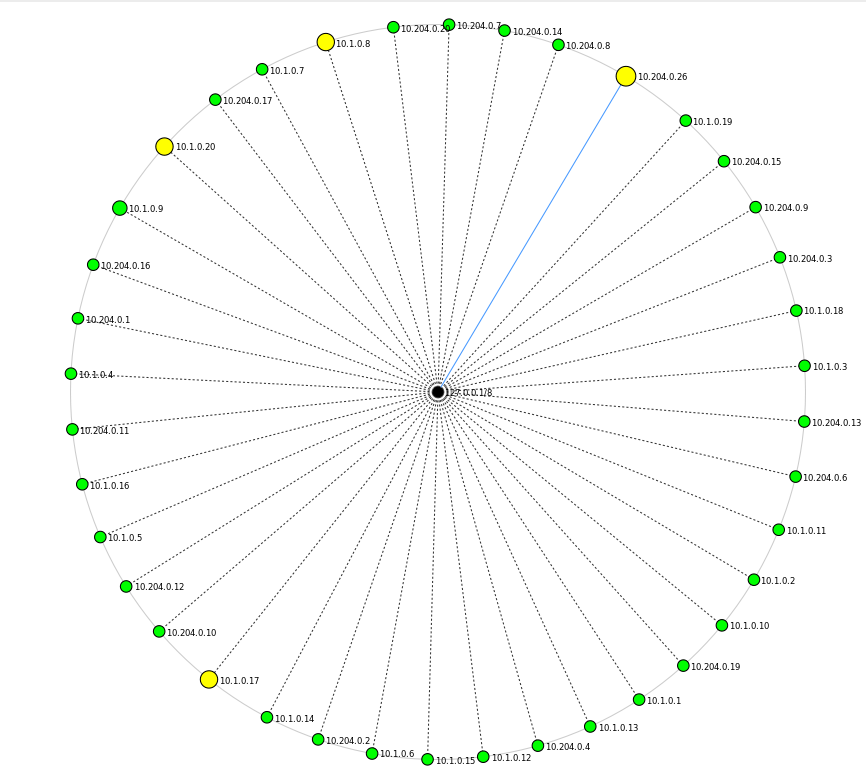
* 1. Describe how the use of decoys is different than nmap’s idle scanning.
* A decoy scan utilizes a sequence of fake/”decoy” IP addresses to hide the true source IP, while still allowing some TCP responses to return to the attack source (if the attacker uses their actual IP). An nmap idle scan uses a source IP of a “zombie” machine on the target’s network. The attacker will receive no replies directly from the Target, but will learn the port information by probing the zombie again and comparing results.  
  1. Inspect the Wireshark output of your decoy scan. Describe when and how many decoys are sent per real packet.
* The real packet is the third packet sent to a given port (2 decoys, 1 real, 1 decoy per port). There are 3 decoys per 1 real packet because the list of decoy source addresses includes 3 decoys and 1 real IP address.



1. Scan the IP addresses 10.1.0.1 through 10.1.0.20 looking just for FTP, SSH, or web servers. In the interest of time, I suggest running a simple SYN scan using aggressive timing without OS or version detection. Provide a screenshot showing the topology map generated by nmap. Ensure the text is readable. You may want to uncheck the hostname option in the controls panel to remove the clutter; displaying just IP addresses is fine.



* Topology shown on next page.



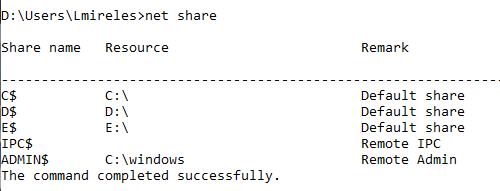
**Shares**

Both team members perform the following, but only provide answers from one member. Provide a screenshot of your results.

Using a command shell, answer the following:

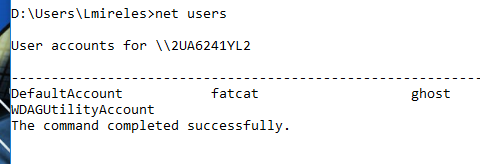
1. List all (including hidden) shares offered on your local machine.

* The shares are C, D, E, IPC, and ADMIN, all of which are hidden as indicated by the $ after the Share name.



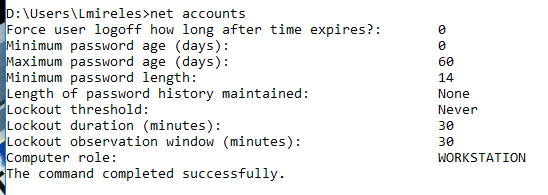
1. List the users on your local machine.

* The users are DefaultAccount, fatcat, ghost, and WDAGUtilityAccount

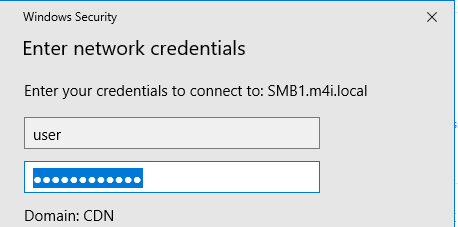


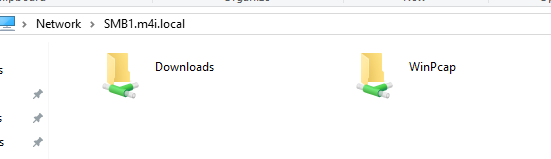
1. List the account settings on your local machine.

* The account settings are shown below:

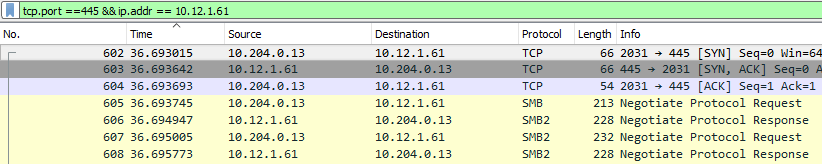


1. Using Server Message Block (SMB) and Windows Explorer, connect to the machine called SMB#.m4i.local where # is your team number. Provide screenshots of the windows/commands used. Which folders are being shared? What transport protocol and port is the SMB server using? Provide a Wireshark screenshot of your computer using the protocol and port listed; filter your Wireshark capture to only include frames involved. What is the secret message found on the target?

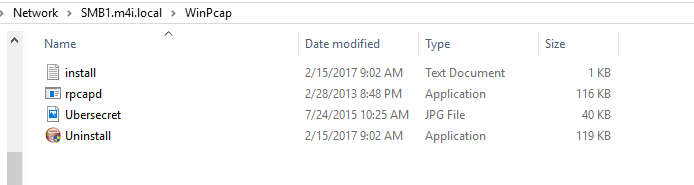
* First we opened Windows Explorer and entered [\\SMB1.m4i.local](file:///\\SMB1.m4i.local)
* This prompted a window asking for the network credentials, and we entered username – “user”, password – “Password!123”
* The following folders are shared on the machine, “Downloads” and “WinPcap”

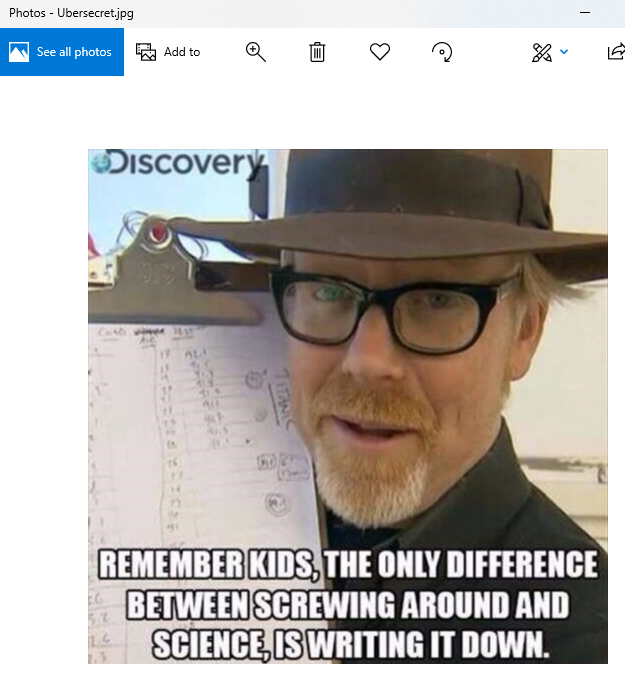


* The SMB server uses TCP on port 445, as shown by the below, filtered Wireshark capture.



* The secret message is below, found by investigating the contents of the machine’s drives:





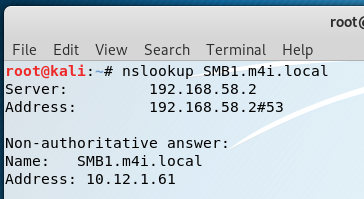
**Extended Reconnaissance and Scanning:**

1. The Air Force has developed a new cyber attack tool. Your assignment is to find the phrase used to activate the tool. This phrase is contained in a file with a name starting with “flag”. In answering each step, provide detailed instructions or commands used as well as screenshots for each step. In order to actually view the file, you are only authorized to use a command shell; you may not use any other Windows utilities like Windows Explorer. At this point in the course, I do not expect you to crack passwords; therefore, I provide the following hints:

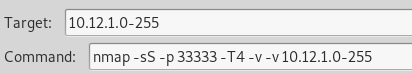
* This computer is on the same subnet as SMB#.m4i.local computers.
* Users are lazy and often use a password that is the same as their username or one of the top 10 worst passwords.
* The cyber attack tool installation process created a listening socket on TCP/33333.
* The following accounts are typical for Windows systems are not of interest for this lab: Administrator, Guest, HelpAssistant, and any account with “Support” in the name.

**Steps:**

1. We performed an nslookup of SMB1.m4i.local to determine IP address to limit subnet IP addresses.

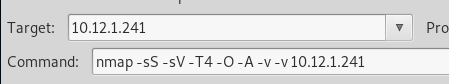
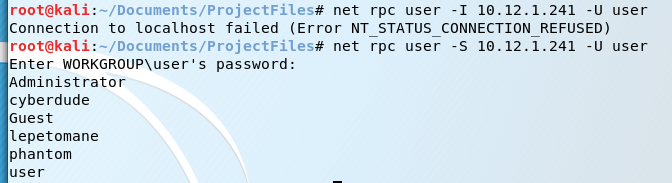


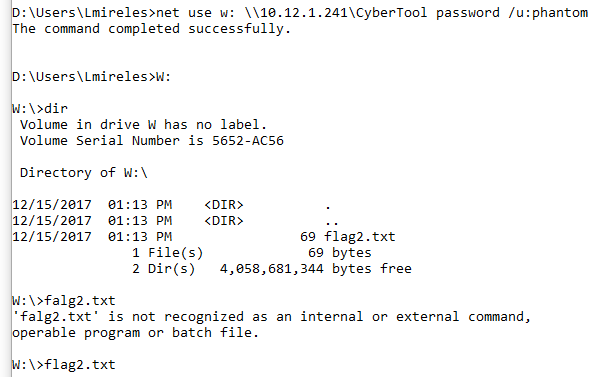
1. We performed an NMap sweep of IP addresses 10.12.1.0-255 searching for an open TCP port 33333.



Found one device with an open port: IP 10.12.1.241.



1. Performed nmap scan of device 10.12.1.241 to learn device details, with results shown with question a below:  
   
2. Ran an smbmap with username – user, password – user on device 10.12.1.241 to find shares:
3. Copied shares to local drives to check files: access was denied to each share using same credentials.
4. Used net rpc user to find list of users on device (tried with –I instead of –S and received an error):
5. Copied Shares to local drives to check files
6. Searched/found Flag2.txt



**Questions:**

* 1. What is the name, IP address, and operating system (and version) of this mysterious computer?

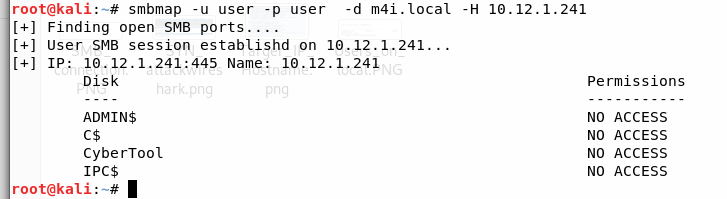
- Result of nmap scan to find device with open port 33333 on subnet:



- nmap scan of device:

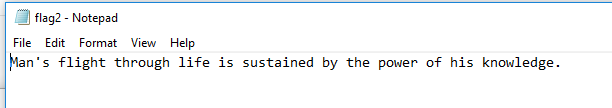


* + 1. Name – AFCyberTool
    2. IP Address – 10.12.1.241
    3. Operating System and Version – Windows 7 Enterprise 7601 Service Pack 1
  1. Identify shares on this machine. Provide a screenshot of your results.
     1. ADMIN$, C$, CyberTool, IPC$



* 1. Find the secret phrase contained in the file located in the shared folder. List the exact instructions you used to find your answer. Provide a screenshot showing the phrase.

The secret phrase is contained in flag2.txt - “Man’s flight through life is sustained by the power of his knowledge”, the exact steps used to find the flag were detailed on the previous page.



**General Observations:**

How long did it take you to complete the lab?

* 5 hours

Was it an appropriate length lab?

* Yes, the time was all productive learning how to solve the various challenges.

What corrections and or improvements do you suggest for this lab? Please be very specific, and if you add new material, provide the exact wording and instructions you would give to future students in the new lab handout. You may cross out and edit the text of the lab on previous pages to make minor corrections/suggestions.

* The exact command used to find the user list to gain access to the shares for question 12 was not found in the slides. We’re not sure if we missed it in class/if there was an alternate method that would have worked, but a significant amount of time was spent gaining access to the shares after profiling the device.